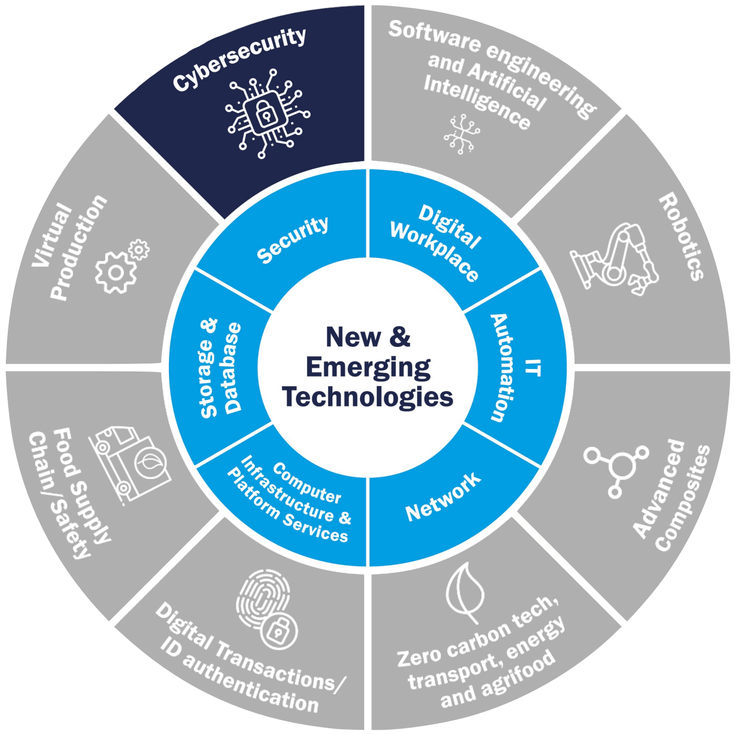


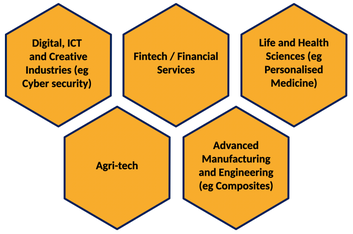
Sources	World Economic Forum	Date	May 2021

Potential scale of impact	Certainty of outcome	Impact horizon
★★★★	★★★★	H1 H2 H3

The recent hack of network management company SolarWinds, which enabled bad actors to compromise a range of US government agencies and major corporations, has revealed a troubling truth: business and government expose each other to significant cyber-risks because they are interconnected and rely on the same network of software vendors. That's why the strategic response must involve more intense collaboration. Simply put, the threat of cyberattacks is too big a job for either government or business to tackle alone.

There are four ways that government and business can join forces

- Share threat intelligence: Governments and companies have different sources of intelligence. Pooling them will create a clearer and more current picture of cyberthreats. The NCSC operates a Cyber Security Information Sharing Partnership with industry, while CISA has similar partnerships with US operators of critical infrastructure.
- Align cyber education with market need: Governments, companies and other institutions around the world face a shortage of cybersecurity professionals. The challenge is twofold: attracting more people to retrain in cybersecurity, and ensuring that curricula enable students to keep pace with fast-changing threats. The NCSC has created CyberFirst to attract young people to the field. More efforts are needed, though, to plug the talent gap.
- Sharpen incident-response capabilities: CISA's National Cyber Incident Response Plan defines cyber defence as a "shared responsibility" of individuals, private sector and government. It spells out the roles government departments will play in responding to attacks and commits officials to safeguarding the privacy and intellectual property of companies. NCSC coordinates similar responses and sets out which private-sector cyber specialists it will collaborate with.
- Build security by design: Human error, such as falling for a phishing attack and downloading malware, is involved in 95% of successful cyberattacks. We can't eliminate that vulnerability, but we should be able to reduce it by building better security into technology devices in the first place – something many tech firms overlook or ignore in the rush to bring new products and services to market.



TOO BIG A JOB

Governments and business need to pool resources to put up effective cybersecurity defences

Home Page
www.10xhorizonscan.online